

Service Name

AWS IoT Core

Service Overview

AWS IoT Core is a managed cloud service that enables connected devices to securely interact with cloud applications and other devices. It acts as a central hub for bi-directional communication between IoT devices and AWS services, supporting billions of devices and trillions of messages. The service provides device gateway capabilities, message broker functionality, and secure device management features including authentication, authorization, and encrypted communication using TLS protocols. AWS IoT Core processes and routes messages to AWS endpoints and other devices reliably and securely while offering features like device shadows for offline state management and rules engine for data processing and routing.

Key Use Cases

- **Connected home automation:** Smart devices, appliances, security systems, and voice-enabled products with Alexa integration for home automation and monitoring
- **Industrial IoT and predictive maintenance:** Asset condition monitoring, predictive quality analytics, equipment performance optimization, and process automation for manufacturing and industrial environments
- **Vehicle connectivity and fleet management:** Connected mobility solutions for automotive applications, vehicle data collection, telematics, and fleet monitoring with real-time analytics

Features

- **Device Gateway:** Secure bi-directional communication bridge between IoT devices and AWS IoT Core supporting MQTT, HTTP, and WebSocket protocols
- **Message Broker:** Scalable messaging service for real-time communication between devices and AWS services with MQTT protocol support
- **Device Shadow:** Virtual representation of devices maintaining state information for online/offline communication and synchronization
- **Rules Engine:** SQL-like service for filtering, transforming, and routing device data to other AWS services and external endpoints
- **Thing Registry:** Device metadata database storing certificates, attributes, and thing types for organized device management
- **Authentication and Authorization:** Fine-grained security with X.509 certificates, IAM integration, and IoT policies for secure device access
- **LoRaWAN Support:** Managed LoRaWAN Network Server for low-power, long-range connectivity with public and private network support

- **Device Advisor:** Testing service for validating IoT devices before deployment with compatibility and capability assessments

Value Proposition

AWS IoT Core offers unmatched scalability supporting billions of devices and trillions of messages with global availability across 20+ regions. The service provides enterprise-grade security with end-to-end encryption, certificate-based authentication, and fine-grained access controls:

- Its fully managed nature eliminates infrastructure management overhead while offering seamless integration with 20+ AWS services including Lambda, S3, DynamoDB, Kinesis, and analytics services
- The pay-as-you-use pricing model with generous free tier makes it cost-effective for any scale
- Advanced features like message enrichment, device shadows for offline scenarios, and comprehensive SDKs across multiple languages accelerate development while ensuring reliability and performance

Service Integration

AWS IoT Core integrates natively with over 20 AWS services through its Rules Engine. Primary integrations include AWS Lambda for serverless computing, Amazon S3 for data storage, Amazon DynamoDB for NoSQL database operations, and Amazon Kinesis for real-time data streaming:

- Additional integrations encompass Amazon SNS for notifications, Amazon SQS for message queuing, AWS Step Functions for workflow automation, Amazon CloudWatch for monitoring, AWS IoT Analytics for data analysis, Amazon Timestream for time-series data, and Amazon API Gateway for REST APIs
- The service also connects to Amazon Elasticsearch, AWS IoT Events for event detection, and supports external HTTP endpoints and Apache Kafka clusters for hybrid architectures

Onboarding and Offboarding

Customers begin by setting up an AWS account and accessing the AWS IoT console. The onboarding process involves creating a ‘thing’ object to represent the device, generating and downloading security certificates and keys, configuring device policies for access permissions, and installing AWS IoT Device SDKs on target devices:

- AWS provides multiple getting-started paths including quick connect tutorials for immediate hands-on experience, interactive demos requiring no physical devices, and comprehensive developer tutorials with detailed explanations
- Device Advisor helps validate device compatibility before production deployment

- The service offers extensive documentation, code examples across multiple programming languages, and SDKs supporting C++, Python, JavaScript, Java, and embedded systems

Getting Started Guide: <https://docs.aws.amazon.com/iot/latest/developerguide/iot-gs.html>

Data Removal

Offboarding requires systematic removal of IoT resources including deleting thing objects, revoking and deleting device certificates, removing device policies and thing groups, and clearing device shadow data. Customers should disable rules engine configurations, delete custom authorizers, and remove IoT jobs before account closure. All data stored in integrated AWS services like S3 buckets, DynamoDB tables, and CloudWatch logs must be separately deleted as these are not automatically removed when IoT Core resources are deleted.

Backup/Restore and Disaster Recovery

AWS IoT Core provides disaster recovery through cross-region replication of device registry, certificates, and policies using DynamoDB Global Tables and Lambda functions. Device shadows and thing metadata can be automatically replicated to secondary regions. AWS offers a dedicated Disaster Recovery for AWS IoT solution using Step Functions workflows for automated failover. The service leverages Route 53 health checks for automatic region failover and supports backup strategies through AWS Backup integration for connected services.

Backup Capabilities

AWS IoT Core does not directly integrate with AWS Backup service. Backup capabilities exist through replication of device registry data, certificates, and policies to secondary regions using DynamoDB streams and Lambda functions:

- Device shadow state and thing metadata can be backed up through custom solutions
- Connected AWS services like S3, DynamoDB, and CloudWatch that store IoT data can utilize AWS Backup for comprehensive data protection strategies

Disaster Recovery

AWS IoT Core does not directly integrate with AWS Elastic Disaster Recovery service. However, it provides disaster recovery capabilities through multi-region architecture, cross-region replication of device registry and certificates, and automated failover using Route 53 health checks. AWS offers a dedicated IoT disaster recovery solution using Step Functions and DynamoDB Global Tables for real-time replication and automated recovery procedures.

Recovery Objectives

AWS IoT Core supports RPO and RTO objectives through multi-region deployment strategies. Cross-region replication of device registry and certificates provides near real-time data protection with RPO of minutes. Automated failover using Route 53 and health checks can achieve RTO of 2-4 hours for backup/restore strategies. For critical workloads, warm standby or multi-site active/active architectures can deliver sub-hour RTO requirements while maintaining low RPO through continuous replication.

Service Constraints

Service Quotas: <https://docs.aws.amazon.com/general/latest/gr/iot-core.html>

FAQ: <https://aws.amazon.com/iot-core/faqs/>

Technical Requirements

Service Documentation: <https://docs.aws.amazon.com/iot/latest/developerguide/what-is-aws-iot.html>

User Guide: <https://docs.aws.amazon.com/iot/latest/developerguide/iot-gs.html>

API Reference: <https://docs.aws.amazon.com/iot/latest/apireference/>

Pricing Overview

Please see the AWS UK G Cloud 15 Pricing Document accompanying this service in the Digital Marketplace.

Public Pricing: <https://aws.amazon.com/iot-core/pricing/>

Cost Optimization

AWS IoT Core offers multiple cost optimization strategies including efficient message batching to reduce per-message costs, Basic Ingest feature for free message ingestion when using reserved topics, and payload compression to minimize data transfer charges. Device connection optimization through persistent sessions reduces reconnection overhead:

- Strategic use of device shadows minimizes frequent state updates, while Rules Engine filtering reduces downstream service calls
- The free tier provides 2.25M connection minutes, 500K messages, and 225K registry operations monthly
- Organizations can leverage LoRaWAN for low-cost, low-power connectivity and implement edge processing with IoT Greengrass to reduce cloud data transfer costs

Savings Considerations

Primary cost savings opportunities include utilizing the 12-month free tier effectively, implementing message compression and batching strategies, and optimizing device connection patterns to minimize connection time charges. Basic Ingest provides free message processing when using specific topic formats:

- Edge computing with AWS IoT Greengrass reduces cloud processing costs by handling data locally
- Strategic data retention policies and lifecycle management for stored IoT data in S3 and DynamoDB minimize long-term storage costs
- Monitoring usage patterns through Cost Explorer helps identify optimization opportunities, while right-sizing concurrent connections and message frequencies based on actual requirements prevents over-provisioning charges